Technical Information

TI 36J04B11-01E

Achieving 21 CFR Part11
Compliance using Exaquantum/Batch
Authored by **Stelex**

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan
Tel.: 81-422-52-6375 Fax.: 81-422-52-5994

Blank Page

Introduction

This document is a white paper written by Stelex, the pharmaceutical consulting firm in the United States objectively evaluating how the Exaquantum/Batch (R2.50) satisfies the FDA 21 CFR Part 11 requirements, the regulation by United States Food and Drug dministration (FDA).

This document will help users construct a system compliant with the 21 CFR Part 11 by using Exaquantum/Batch.

Trademarks

Blank Page

Achieving 21 CFR Part11 Compliance using Exaquantum/Batch Authored by Stelex

TI 36J04B11-01E

CONTENTS

Blank Page

YOKOGAWA

Exaquantum/Batch

Achieving 21 CFR § 11 Compliance using Exaquantum/Batch

Authored by: stelex
A Xybion Company

SYNOPSIS

This paper will provide a detailed discussion of Yokogawa's Exaquantum/Batch (R2.50) Plant Information Management System and Yokogawa's efforts to enable Exaquantum/Batch installations to comply with 21 CFR Part 11, including the Guidance for Industry Part 11, Electronic Records; Electronic Signatures – Scope and Application (August 2003). The focus will include the compliance aspects of software solutions employed to enhance the functionality and compliance of Exaquantum/Batch. The measures to be implemented by the purchaser of such solutions will also be discussed. Included in the discussion will be the policies, procedures and best practices for achieving maximum compliance and recommendations for customers and integrators in implementing the applications within FDA-regulated environments.

I. Introduction: What is 21 CFR Part 11?

The pharmaceutical industry recognizes that the implementation of paperless systems can provide a wide variety of benefits including, among other things, increased speed of information exchange, and improved ability to integrate, trend, search and retrieve batch and other production related data. These improvements can lead to a reduction in both errors and costs related to data storage and, ultimately, to improved quality and efficacy of product.

During the 1990's, the pharmaceutical industry sought guidance from the U.S. Food and Drug Administration (FDA) in the development of a uniform approach to the acceptance of paperless systems. As a result, the FDA issued its Final Rule on electronic records and electronic signatures ("21 CFR Part 11," "Part 11," or "the rule") on March 20, 1997; the rule took effect on August 20, 1997.

Part 11 establishes the criteria under which electronic records and electronic signatures are considered as equivalent to paper records and handwritten signatures executed on paper. The rule applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations. In addition, documents submitted to the FDA but not necessarily required by federal regulation also fall under the requirements of the rule. Part 11 does not apply to paper records transmitted by electronic means, such as by fax. Currently the FDA will accept electronic submissions of documents (in whole or part) that are identified in Public Docket 92S-0251 as being the type of submission the agency accepts in electronic form.

Those forms include:

- Biologics License Applications (BLA)
- Product License Applications (PLA)
- Establishment License Applications (ELA)
- New Drug Applications (NDA)
- Abbreviated New Drug Applications (ANDA)
- Biologics Marketing Applications
- Post marketing Expedited and Periodic Individual Case Safety Reports (ICSRs)
- Advertisements and Promotional Labeling
- Basic Information re Submission of Notices of Claimed Investigational Exemption to Center for Veterinary Medicine (CVM).
- Food and Color Additive Petitions

The list of accepted electronic submissions in Public Docket 92S-0251 has increased significantly in the recent past and will continue to do so. (For example, FDA began accepting electronic submissions for Investigational New Drug Applications [NDAs] as of September 30, 2002.)

Definitions in 21 CFR Part 11

Biometrics (21 CFR § 11.3(b)(3)): A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
Closed System (21 CFR § 11.3(b)(4)): An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
Digital Signature (21 CFR § 11.3(b)(5)): An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
Electronic Record (21 CFR § 11.3(b)(6)): Any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature (21 CFR § 11.3(b)(7)): A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
Handwritten Signature (21 CFR § 11.3(b)(8)): The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form.
Open System (21 CFR § 11.3(b)(9)): An environment in which system access is *not* controlled by persons who are responsible for the content of electronic records that are on the system.

Definition Of Terms

SQL: SQL (Structured Query Language) is a standard interactive and programming language for getting information from and updating a database.
I.P: The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.
ODBC: (Open Database Connectivity) is a standard method of sharing data between databases and other programs.
OPC: A set of open standards for connectivity and interoperability of industrial automation and enterprise systems published by the OPC Foundation. Yokogawa is a leading member of the OPC Foundation.

General Requirements of 21 CFR Part 11

In order for organizations to comply with Part 11, a number of requirements must be met. These requirements generally concern the authenticity, integrity and confidentiality of the electronic records and signatures. Any computer system utilizing electronic records and signatures should be validated according to generally accepted industry standards associated with a software development life cycle, to ensure its accuracy, reliability, consistent intended performance, and ability to discern invalid or altered records. Software validation is defined by the FDA as "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled" (Ref: FDA, General Principles of Software Validation; Final Guidance for Industry and Staff, January 11, 2002). The system must be able to generate copies in both human readable (i.e., in plain text) and electronic form that are accurate and complete.

Several types of checks must be built into Part 11 compliant systems including:

- Operational System checks that enforce the sequencing of events, as appropriate
- Authority checks that determine who has access to the system and at what level
- Device checks that determine the validity of sources of data being entered into a system, as appropriate

Organizations using electronic records must also limit system access to authorized individuals. This requires a policy regarding the levels of access, the roster of individuals within each level, the criteria for determining eligibility to that level, and other system safeguards to prevent access to records by unauthorized individuals.

As with most FDA regulations, including most predicate rules, Part 11 requires that individuals who develop, maintain, or use electronic record and electronic signature systems, have the education, training, and experience to perform their assigned tasks.

II. Recent changes in FDA's Thinking Regarding Scope and Application of Part 11

On February 20, 2003, the FDA issued for comment a draft guidance document designed to address industry concerns, clarify the scope of part 11, and describe interim changes to their part 11 enforcement policy. The FDA withdrew all part 11 draft guidance documents, including those on Validation, Glossary of Terms, Time Stamps, Maintenance of Electronic Records, and Electronic Copies of Electronic Records. The FDA withdrew Compliance Policy Guide 7153.17, as well.

During the subsequent comment period, FDA reviewed the concerns that had been raised. The August 2003 guidance concerning scope and application of Part 11, published on September 3, 2003, addresses industry concerns and represents the FDA's latest thinking on both part 11 interpretations and enforcement intentions.

Under the new interpretation, four classes of electronic records fall under the scope of part 11: (1) electronic records that will be submitted to the FDA even if they are not specifically required by Agency regulations to be submitted, (2) records maintained electronically ***in place of paper format*** and are required to

be maintained by predicate rules, (3) records maintained electronically ***in addition to paper format*** and ***are relied on to perform regulated activities***, and (4) electronic signatures that are intended to be the equivalent of handwritten signatures, initials, and other general signings required by predicate rules.

Electronic records that are incidentally created in the course of developing a paper record (e.g. using a word processor application to create an SOP based on an existing SOP template that will be generated, printed, approved, and used in paper form without using the electronic form for any regulated purpose) would generally not fall under the scope of part 11.

In the new guidance, the FDA has made it clear that they are in the process of revising current Good Manufacturing Practice (cGMP) for pharmaceutical products, and that they intend to begin rulemaking to revise portions of part 11 as part of that process. The guidance describes the FDA's intention to "exercise enforcement discretion with regard to part 11 requirements for validation, audit trail, record retention, and record copying" during this revision process. Also, the FDA intends to "enforce all other provisions of Part 11 including, but not limited to, certain controls for closed systems in § 11.10. For example, we intend to enforce provisions related to the following controls and requirements:

- limiting system access to authorized individuals
- use of operational system checks
- use of authority checks
- use of device checks
- determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- appropriate controls over systems documentation
- controls for open systems corresponding to controls for closed systems bulleted above
- requirements related to electronic signatures

FDA indicated that it would not re-issue the draft guidance documents or the Compliance Policy Guide. However, FDA stated that their current thinking on time stamps has not changed, in that when using time stamps for systems that

span different time zones, that times should be recorded relative to a standard time zone and not recorded as the signer's local time.

Further, it is clear in the draft guidance that the FDA views the security and integrity of electronic data as critical in achieving compliance with part 11 and predicate rules.

Electronic Signatures – Requirements

Part 11 sets forth general requirements for organizations that intend to use electronic signatures. Each electronic signature used within an organization must be unique to an individual and not reused or assigned to another individual. The identity of the individual must be verified by the organization (e.g., via birth certificate, driver's license, passport) before assigning the individual an electronic signature. The organization must also certify in writing to the FDA that they intend to use their electronic signatures as the legally binding equivalent of their handwritten signatures; that certification must be submitted to the FDA in paper form. If required by the FDA, the organization may be required to submit additional certification that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

Biometric and non-biometric electronic signatures must exhibit certain characteristics reflective of their nature. Biometric electronic signatures must be designed to ensure that they cannot be used by anyone other than their genuine owners. Non-biometric electronic signatures must be composed of at least two distinct identification components (e.g., user ID and password); must be used only by their genuine owners; and must be administered and executed such that two or more individuals are necessary to attempt to use another user's signature. Non-biometric electronic signatures also have specific requirements for use during periods of controlled access. If an individual executes a series of signings during a single period of controlled access, they must use all electronic signature components for the first signing and at least one electronic signature component for each subsequent signing, the one that is executable only by the individual. If, however, signings are not performed during a single period of controlled access, each signing must use all electronic signature components.

Signature Manifestations and Linking

Part 11 requires that signed electronic records bear a signature manifestation, that is, a clear indication of the printed name of the signer; the date and time of the signing; and the meaning of the signing. Those records are subject to the

same controls as electronic records, and must be available as part of the entire record for review and copying by the agency. Electronic signatures, as well as handwritten signatures executed to electronic records, must be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

III. What is Yokogawa Doing?

Yokogawa has a long and substantial history as a world leader in industrial automation and control, test and measurement, information systems, and industry support. Yokogawa has secured more than 4,500 patents and registrations, representing a number of important innovations, including the world's first distributed control system and the first digital sensors for flow and pressure measurement.

In July 2003, Yokogawa contracted with Stelex to perform an evaluation of Exaquantum/Batch. Exaquantum/Batch is a valuable tool in batch-orientated industries allowing business benefits to customers in the Hydrocarbons, Pulp & Paper, Power & Utilities, Chemicals, Pharmaceuticals, Food & Drink, Manufacturing and other continuous or batch processing industries to focus on Key Process Performance Indicators. It provides a web browser based analysis and reporting user interface to deliver batch information in support of process improvement initiatives. This is achieved by integrating data from all facets of the business and transforming these into usable, high-value business information as part of the enterprise's vital decision support toolset. Stelex performed the evaluation by assessing the applicability of Part 11 to the application. Key assumptions made during the evaluation were (1) the applications need to comply with all requirements of Part 11; and (2) the applications will not be used in open systems as defined in Part 11. A checklist based on the requirements of Part 11 was used, and the application was assessed for the applicability and level of compliance with the rule.

As a result of the assessment and other aforementioned efforts, Yokogawa and Stelex-TVG have proposed a set of recommendations for customers with existing installations on best practices and software solutions to meet the intent of Part 11 regulations.

Best Practices and Software Solutions for Existing Installations

Customers are advised to implement the following practices and software solutions to meet the intent of Part 11 regulations when using Exaquantum/Batch. The recommendations made below provide a solid basis for both compatibility with future releases and compliance with GxP and Part 11. A detailed Part 11 checklist that served as a basis for these recommendations is included in this document.

Application

- Customers in a FDA-regulated environment are advised to use the Exaquantum/Batch application to access batch-related equipment and other points.
- It is further recommended that the use of Exaquantum/Batch be restricted to an intranet or a secure VPN (Virtual Private Network) thus curtailing the possibility of any unauthorized access.

Security

- Customers are advised to configure Exaquantum/Batch to limit system access. Exaquantum/Batch administrators should create accounts for individual users and assign rights that are appropriate with user responsibilities. Users must be required to create passwords and periodically change them. Care should be taken not to delete any user account on the system, but rather to disable or lock the account for the said user when required.
- Customers should use Windows domain security. Domain administrators should implement account policies on password aging, minimum password length, password uniqueness, and account lockout after a reasonable number of unsuccessful login attempts.
- To prevent unauthorized use of passwords, Windows security should be used to disable access after an appropriate number of unsuccessful login attempts. The Windows security engine will log any such events to the event logs, which should be periodically monitored by administrators.
- To limit the duration of a continuous period of controlled system access, a password protected screen saver should be configured to activate after a reasonable inactivity period. Some factors in determining the appropriate length of the inactivity period include the accessibility of the computer or terminal to non-authorized personnel and the number of potential computer or terminal users.

- To ensure the validity of the source of data input, customers must ensure that all computers or terminals are placed in secure locations and that access to the computers or terminals is limited to authorized personnel.

Electronic Records/Electronic Signatures

- To ensure protection of records throughout the records retention period, customers should implement one or more of the following measures:
- Customers are advised to ensure that the SQL database is located on a secure machine and access to this machine is limited to authorized personnel only. This can be achieved by restricting both physical and logical access to the database with procedures to ensure that data is not transferred, changed or edited by unauthorized personnel.
- Customers are also advised not to delete the Event log. The delete function erases the data contained in the Event log. It is recommended that change control procedures be developed to ensure that the data is archived in an appropriate manner (to be retrieved at a later date, if necessary) before the delete function is utilized. This functionality should be made available only to the system administrators.
- To deter tampering and to determine the validity of the source of data input customers are advised to configure the Exaquantum/Batch to connect to only known I.P. addresses for circuit monitors in the field. This can be verified during the setup of the systems that will be monitored by the Exaquantum/Batch.

Validation and Documentation

- Many of the requirements of the rule must be met by practices that are not software-based. In order to meet the validation requirement of Part 11, customers must validate the Exaquantum/Batch in order to ensure accuracy, reliability, consistent and intended performance, and the ability to discern invalid or altered records. Customers may develop and/or execute the validation plans and protocols themselves or outsource these activities. The validation should follow an established system life cycle (SLC) methodology.
- To enable accurate and ready retrieval of Exaquantum/Batch records throughout the records retention period, customers are advised to create procedures outlining record retention periods, archival and retrieval policies.
- In order to meet the authority checks requirement of the rule, customers must establish and adhere to policies and procedures to verify the identity of the individual to whom an electronic signature will be issued.
- Customers must establish and adhere to written policies that hold individuals accountable and responsible for actions initiated under their electronic

signatures in order to deter record and signature falsification and to meet that requirement of the rule.
- Although customers are not responsible for control over the content of system operation and maintenance manuals, they should be responsible for establishing and maintaining controls over the distribution of, access to, and use of that documentation as required by Part 11.
- Customers must verify the identity of the individual before assigning an electronic signature to him/her. Customers are also responsible for certifying in writing (in paper form with traditional handwritten signature) to FDA that they intend to use their electronic signature as the legally binding equivalent of their handwritten signature and, if necessary, submit additional certification of that intention to the agency for a specific electronic signature.
- Customers should implement policies and procedures requiring users to log out of the application during periods of non-use.
- Customers must create procedures for ensuring that identification code and password issuances are periodically checked, recalled, or revised.

Miscellaneous
- Access to Exaquantum/Batch should not be available from an open system (i.e. over the Internet). This can be achieved by allowing access to the software only via secure intranet or a Virtual Private Network (VPN) which has been validated to ensure the security and integrity of the data transfer mechanism.

Product Description

Exaquantum/Batch is a smart and scaleable S88 based Batch PIMS (Plant Information Management System). It provides an analysis and reporting application that collects, stores and displays current and historical data from batch production, equipment and recipe viewpoints. This enables production, recipe management, process engineering and operations staff to easily access batch production information for decision support, production planning and scheduling, analysis, process improvement and quality purposes.

Exaquantum/Batch focuses on KPIs (Key Performance Indicators) using the web based browsing, analysis and reporting user interface. This enables customers to develop action plans for process improvements.

Exaquantum/Batch's "Out of the box" functionality provides automatic collection of batch data, thereby freeing users from having to build queries and displays to obtain and then view the data.

As batch data is collected it is immediately available for display in BatchWeb, the web based user interface, in a number of standard views available for displaying batch, equipment and master recipe information. Batch and product performance data is also automatically calculated and available for display.

Features

The key features of Exaquantum/Batch are:

- Automatic Batch Data & Master Recipe collection
  - Minimizes setup time and engineering
- Custom Batch Data collection
  - For any control/MES system with an OPC Data Access 2.0 server
  - Primary data source or may augment automatic batch data collection
- Web based user interface
  - Standard display structure based upon S88
  - Batch trends, Gantt charts, Data filtering
  - Standard cycle time analysis displays
  - Secure access to data
  - Access data from any intranet capable PC
- Strong batch reporting platform
  - Batch, master recipe & equipment data available for any report
  - Custom reports
  - No artificial limits to the number of data items in a report
  - Reports may contain any information stored in Exaquantum/Batch
- Standard analysis calculations & charts
  - Cycle time & batch performance metrics automatically maintained
- Meeting demands for standards based solutions
  - Based upon S88 models & terminology
  - OPC Batch, Data Access and Alarms & Events
  - FDA 21 CFR Part 11
- High level batch solutions coupled with batch control system
  - Traditional Time & Tag based PIMS no longer sufficient for batch solutions
  - High performance & reasonable cost

Exaquantum/Batch Part 11 Support Highlights - Electronic Records

Exaquantum/Batch stores all configuration and operational data in a relational database. Each customer must decide which data stored in the database will be considered electronic records in their application. Typical examples of data considered electronic records are:

- Final batch data including control recipe header, equipment, formula values and record of the unit recipes and operations run as part of the batch.
- A copy of the master recipe used to create the batch's control recipe.
- A record of the events associated with a batch.
- Trend data from instrumentation used to produce a batch.
- A record of the equipment organization in effect when the batch was run.
- Report output containing subsets of the above data.

Exaquantum/Batch is designed to provide secure storage of electronic data. Access to the Exaquantum/Batch database is controlled using Windows domain security.

Most of the data written to the database is done by collection programs, which must be validated to assure that electronic records are accurate, reliable and consistent.

When an operator modifies data, an electronic signature must be applied for each change. Changes are also recorded in the audit trail. This enables customers to discern invalid and altered records.

Availability of Electronic Records

Since Exaquantum/Batch stores all electronic records in an Open Database Connectivity (ODBC) compliant database they are available using the BatchWeb client, Report Package and many 3rd party software packages.

Using server class computers and advanced disk storage devices, the Exaquantum/Batch server can offer high reliability and make many years of data available on-line. If desired, database administrators can store older data off-line thereby reducing the size of the on-line database.

Using Windows security, individual users may be given read-only access to the database to produce reports and extract data. Use of this security feature assures that users extracting data cannot alter any of the electronic records.

Audit Trail

Exaquantum/Batch maintains a record of operator entries and actions as well as many system events. Depending upon the type of change, action or event, the data is stored in one of the following:

- Exaquantum/Batch audit trail,
- Exaquantum/Batch property history table, or
- Windows event log.

The Exaquantum/Batch audit trail maintains a record of all operator entries and approvals made using BatchWeb.

The audit trail contains the following information:

- Time stamp
- Computer name where the entry or action occurred
- The full name associated with the Windows user account
- Identification of the changed item in the database
- Reason for the change as entered by the operator
- Previously recorded value
- Entered value or action
- Identification of the entry as creation of a new item or modification of an existing item.

The Exaquantum/Batch property history table is used to record changes to property values made by the collection programs. For example if a batch's estimated end time property was changed during the batch, the most recent value is available in the database and all previous values of the property are preserved, not overwritten, in the property history table. This data is available in reports and to the database administrator. The property history table contains the following information:

- Time stamp
- Identification of the data that was changed
- Old value
- New value
- Identification if the change represents a new item or a modified item

The name of the user is not recorded since all the data in this table records changes made by collection programs, not users.

The Windows event log is used to record Exaquantum/Batch program events such as the start and stop of programs or services, program errors dealing with the operating system environment, and other significant program events. This log is not used for operational data, rather it is intended to provide trouble shooting assistance to system administrators, although auditors may also be interested in some of the records. The event log is viewed using the Windows Event Viewer, which is a standard component of the Windows operating system. The event log size may be adjusted, however whenever the event log is full, older entries are removed from the log and are no longer available. Therefore system administrators should periodically save the contents of the log as an archive.

Electronic Signature Support

Exaquantum/Batch supports the use of electronic signatures for approving specific types of electronic records. Windows user name and password are used to apply electronic signatures.

If a company or manufacturing site does not utilize electronic signatures for submittal of records to the FDA, the Exaquantum/Batch electronic signature still provides a benefit by providing documented evidence of who made a data entry, approved a template for use, or approved a report output.

Exaquantum/Batch's electronic signatures have been designed to:

1. Clearly identify to the user that an electronic signature is being entered
2. Require the identification of a user entering data or performing an action
3. Bind the electronic signature to the electronic record
4. Prohibit the copying of electronic signatures using ordinary means
5. Automatically record electronic signatures in an audit trail

The following Exaquantum/Batch actions require an electronic signature:

1. Create new formula items using BatchWeb
2. Modify formula item values using BatchWeb
3. Modify performance rating values using BatchWeb
4. Approve report output using BatchWeb
5. Approve report templates using the Report Template Manager Tool

Exaquantum/Batch preserves the signature manifest data for each electronic signature and treats the data the same as an electronic record. The signature manifest data is displayed in BatchWeb and is available for inclusion on reports.

The following information is preserved for an electronic signature:

1. The full name associated with the Windows user name
2. The date and time the signature was entered
3. The reason for the signature as entered by the user
4. The host name of the computer used to enter the signature
5. The new value and the previous value

The signature manifest data for formula item creation, value changes and performance-rating changes are displayed in BatchWeb. The data is displayed in different fashions depending upon the display. For example in a property sheet the signature manifest data is displayed as property values; when the signed value is in a table, an icon is included in the same cell that provides a hyperlink to call up a signature manifest pop-up window; and when a signed value is included in a chart, a table containing the signature manifest data is provided below the chart.

The signature manifest data for report output approval is available for inclusion in the report output. The design of the corresponding report template determines if the data is included.

The signature manifest data for report template approval is displayed as part of the Report Template Manager tool. This is also available for display on report output based upon the report template design.

Use of Windows Domain and Operating System

Exaquantum/Batch should be used in a Windows domain. The use of the Windows operating system and domain to control access are widely accepted practices in industry. It is assumed that regulated companies have policies and procedures regarding the use of Windows that meet Part 11 requirements.

System Administration

The system administrator role is critical to assuring that a system is secure and data is not altered without authorization and an audit trail or other evidence. Exaquantum/Batch provides safeguards against the unauthorized alteration of

electronic records by ordinary means; however system administrators may have the knowledge and ability to access data at the file system and interactive SQL level. Potentially this could lead to undetected alteration of data. This is a widely recognized issue in industry that requires procedural controls.

While 3rd party security software packages are available for Windows and SQL Server the most common preventive measures involve the separation of authority. For example, administrative privileges can be assigned to individuals who report outside of the manufacturing operations organization. In addition, Exaquantum/Batch system administration responsibilities are divided among different roles with each role assigned to different individuals or groups of people.

The three levels of Exaquantum/Batch administrator roles are:

- Domain administrators
- Database administrators (DBA) and
- Exaquantum/Batch-Exaquantum administrators

The domain administrator is responsible for network security including setting up and maintaining user accounts, user groups, administering Windows group policies, and ensuring there is no unauthorized access to Exaquantum/Batch from beyond the company's domain. This role is usually assigned to an IT group instead of one individual.

The database administrator is responsible for the smooth operation of the Exaquantum/Batch relational database. There is a low level of activity associated with this role in most applications. If there are Yokogawa, 3rd party or user-developed applications on top of Exaquantum/Batch, this role may require additional activity. The primary activities are to perform regular backups of the database, the monitoring of disk space used by the database and the amount of free space available, preparation for disaster recovery, and restoration of backup data as necessary.

The Exaquantum/Batch administrator is responsible for installing, configuring and maintaining Exaquantum/Batch. This involves using the configuration tools to enter data such as OPC server locations, CENTUM CS Batch 3000 or CENTUM VP for Batch Control recipe file locations (if applicable), Custom Batch Data Collection configuration, Exaquantum/Batch Plant View configuration, and monitoring the audit trails.

System Security

Exaquantum/Batch security has been designed to meet the requirements of Part 11. The central point in system security is to control access to Exaquantum/Batch programs and data. This is required to maintain the integrity of the electronic records.

Exaquantum/Batch uses Windows security to enforce access control. Only users with Windows domain accounts that have been granted the appropriate privilege may access Exaquantum/Batch programs and data.

Reports

Reports in Exaquantum/Batch are based on report templates which are created using the Report Template Manager tool supplied with Exaquantum/Batch. Once a report template has been created, it may be configured to run at a set time and date or when a batch completes.

As templates are created and approved, they become available to BatchWeb users in the Report Templates view and may then be selected to run a report. The report output is available in Excel and PDF (Adobe Portable Document Format) file formats.

Once a report has been run, it is then added to the list of reports in the Report Archive view. The Report Archive view consists of a list of previously run reports, which may be viewed in PDF format.

Reports in Excel format may be checked out of BatchWeb for editing and then checked back in provided the report status is either 'Not Approved' or 'Approval N/A'. (This option is disabled when the Part 11 option is enabled for the application).

Detailed findings: Audit Report

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
B/11.10	Controls for closed systems.			
	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall **employ procedures and controls** designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality **of electronic records**, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:			
(a)	**Validation of systems** to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. **NOTE:** The FDA intends to exercise enforcement discretion regarding this requirement for Part 11, though persons must still comply with applicable predicate rule requirements for validation. The FDA recommends that validation be based on a justified and documented risk assessment.	YES		Validation is unique to each Exaquantum/Batch installation and is ultimately the customer's responsibility. Yokogawa Marex (YMX) operates a Quality Management System that complies to the requirements of the International Quality Standard ISO 9001: 2000 and the TickIT Guide, and incorporates industry standard Product Development processes. These processes are documented and reviewed by both internal and external auditors as per the requirements of the ISO 9001 Standard. Yokogawa Marex followed this Quality Management System in the development of Exaquantum/Batch. Exaquantum/Batch has been designed to accurately collect and securely store batch, master recipe and equipment data in a relational database. Access is controlled and operational changes to the data are tracked to provide the ability to discern invalid or altered records.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(b)	The ability to **generate accurate and complete copies of records** in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records. **NOTE:** The FDA intends to exercise enforcement discretion regarding this requirement for Part 11; persons should provide an investigator with reasonable and useful access to records during an inspection ensuring the copying process produces copies that preserve the content and meaning of the record.	YES		All Exaquantum/Batch data is stored in an ODBC compliant relational database. Customers may use a wide variety of software products to extract data from the electronic records for submission to the FDA. The Exaquantum/Batch Report Package is available to generate reports in human readable format. This function permits any data in the database be included in a report, which can be stored as an Acrobat file or printed. System security may be configured so that neither the Report Package nor Microsoft Excel may be used to alter the data in the database.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(c)	**Protection of records** to enable their accurate and ready retrieval throughout the records retention period. **NOTE:** The FDA intends to exercise enforcement discretion regarding this requirement for Part 11. The FDA suggests the decision on how to maintain records be based on predicate rule requirements and on a justified and documented risk assessment.	YES		Exaquantum/Batch is designed to securely store electronic records throughout the record retention period. Records may be preserved in the on-line Exaquantum/Batch database for access by BatchWeb and the Exaquantum/Batch Report Package, moved to an off-line database for access by 3rd party software packages, or backed up for long-term retention. In order to retrieve backed up records, the records must be restored to an Exaquantum/Batch system or loaded into a SQL Server database and 3rd party software packages can be used to retrieve the records. Exaquantum/Batch maintains an archive of all report outputs. The reports are stored in the relational database in Adobe Acrobat format. The report archive can be a valuable tool for the retention of batch reports. Storing them in the database offers additional protection when compared to storing them using an operating system's file system. Long term, off-line, retention of the records must be performed according to the customer's record retention program. This typically includes activities to either periodically migrate the records to current data formats or to maintain the original software programs used to access the data format. By utilizing common data formats and tools such as ODBC relational databases and Adobe Acrobat format files, the ability for customers to access these files over a 20-30 year time period should be enhanced when compared to proprietary file formats.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(d)	**Limiting system access** to authorized individuals.	YES		Exaquantum/Batch utilizes Windows security to limit access. Domain administrators must grant individual users the privilege to access individual components such as BatchWeb, the Report Package, Configuration Tools and the database. The customer is responsible for limiting access to the Exaquantum/Batch server computers.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(e)	**Use of secure, computer-generated, time-stamped audit trails** to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such **audit trail documentation** shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. NOTE: The FDA intends to exercise enforcement discretion regarding this requirement for Part 11, though persons must still comply with applicable predicate rule requirements related to documentation of, for example, date, time, or sequencing of events. FDA states even if no predicate rule exists for this requirement, it may still be important to have audit trails or other security measure to ensure the trustworthiness and reliability of the records.	YES		Exaquantum/Batch automatically maintains a time-stamped audit trail of manual changes to operator entries and actions. The audit trail is stored in the database separate from the operational data. An audit trail entry contains the new and previous value to prevent previously recorded information from being obscured. The audit trail is retained as part of the Exaquantum/Batch database and may be available for as long as the subject electronic records are preserved. The audit trail contains the following information: • Time stamp • Computer name where the entry or action occurred • The full name associated with the Windows user account • Identification of the changed item in the database • Reason for the change as entered by the operator • Previously recorded value • Entered value or action • Identification of the entry as creation of a new item or modification of an existing item. Exaquantum/Batch is a historical information system that automatically collects data. Operator entry of data is primarily intended for the entry of late or manually collected data and the approval of report templates and reports. Access to enter data and make approvals may be totally restricted or limited to specific individuals.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(f)	**Use of operational system checks** to enforce permitted sequencing of steps and events, as appropriate.	YES		Exaquantum/Batch is a historical information system, not a control or manufacturing execution system. Therefore the sequencing of steps and events enforced by Exaquantum/Batch deal with information such as entering data, developing reports or running reports and with the collection of data. Exaquantum/Batch can be configured to require the entry of the users account and password when data is entered manually. Also report templates and outputs must follow a set lifecycle of states that require approvals for a template to be used and for report outputs to be viewed. When Custom Batch Data Collection is used, Exaquantum/Batch sets a handshake value after the data specified in a data collection list has been successfully collected and stored. The handshake may be configured to signal a control or information system application that the data has been collected and the storage locations may be reused in the local application. Exaquantum/Batch by itself does not perform control actions; this would be done in an associated control system such as CENTUM CS Batch 3000 or CENTUM VP for Batch Control.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(g)	**Use of authority checks** to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	YES		Exaquantum/Batch performs authority checks using the current Windows user's login credentials. These credentials include the privileges assigned to the user account by the domain administrator. The specific Exaquantum/Batch privileges are: • Access to view BatchWeb pages • Create new formula items using BatchWeb (Electronic signature may be required) • Modify formula item values using BatchWeb (Electronic signature may be required) • Override individual lockouts to change formula item values using BatchWeb (Electronic signature may be required) • Modify performance rating values using BatchWeb (Electronic signature may be required) • Create, modify and delete batch trend templates using BatchWeb • Run reports using BatchWeb • Access to Windows based configuration tools • Approve report templates (Electronic signature may be required) • Approve report output (Electronic signature may be required) • Check-out/in report output files • Read-only access to the database • Create, read, update and delete access to the database Without the correct privilege granted to their user account a user cannot perform an action. Even with the correct privilege granted to a user account, the system can be configured to require a user to enter an electronic signature to confirm their identity. The privileges that may require an electronic signature are indicated above.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(h)	**Use of device** (e.g., terminal) **checks** to determine, as appropriate, the validity of the source of data input or operational instruction.	YES		There is no restriction based upon physical terminal identification or location. Exaquantum/Batch restricts manual data entry based upon the user's login credentials. A user's Windows account must have previously been granted the privilege to perform an action or make an entry.
(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems **have the education, training, and experience to perform** their assigned tasks.	N/A		Yokogawa's development, marketing and engineering personnel are familiar with 21 CFR Part 11, continue to pursue training in the regulation, meet with regulated companies to learn how it is interpreted and complied with, and track information provides by the FDA regarding the regulations enforcement, interpretation, guidance development and new regulation development. Customers are responsible for the level of education, training and experience of personnel working with regulated systems.
(j)	The **establishment of, and adherence to, written policies** that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order **to deter record and signature falsification**.	N/A		Customers are responsible for establishing and maintaining adherence to policies regarding the use of electronic signatures.
(k)	Use of appropriate controls over **systems documentation** including:			

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(1)	**Adequate controls** over the distribution of, access to, and use of documentation **for system operation and maintenance**.	N/A		Yokogawa maintains control of Exaquantum/Batch documentation as it is developed and maintained. Upon receipt of Exaquantum/Batch documentation customers are responsible for controlling access to the documentation. Customers will need to develop application specific documentation covering the operation and maintenance of the Exaquantum/Batch system. Yokogawa would be pleased to assist customers in developing system specific procedures and documentation.
(2)	**Revision and change control procedures** to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	YES		Exaquantum/Batch documentation is in HTML on-line help format. This means that all BatchWeb users access help files from a central location thereby making control of the documentation easier than controlling multiple electronic and/or paper copies distributed among many individual persons or PCs. Yokogawa controls the development, maintenance and distribution of Exaquantum/Batch documentation within Yokogawa.
B/11.30	Controls for open systems			

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
	Persons who use open systems to create, modify, maintain, or transmit electronic records **shall employ procedures and controls** designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall **include those identified in § 11.10,** as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	N/A		Exaquantum/Batch should be used as a closed system. Access to the Exaquantum/Batch server should be limited to valid members of a Windows domain.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
B/11.50	Signature manifestations			
(a)	**Signed electronic records** shall contain information associated with the signing that clearly indicates all of the following:			

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(1)	The printed name of the signer	YES		Exaquantum/Batch preserves the signature manifest data for each electronic signature and treats the data the same as an electronic record. The signature manifest data is displayed in BatchWeb and is available for inclusion on reports. The following information is preserved for an electronic signature: • The full name associated with the Windows user name, • The date and time the signature was entered, • The reason for the signature as entered by the user, • The host name of the computer used to enter the signature, • The new value and the previous value. Electronic signatures are required for the following actions: 1. Modify a formula items value 2. Add a new formula item to a batch, unit recipe or operation 3. Modify a performance rating for a batch or unit recipe 4. Approve a report template 5. Approve a report output The signature manifest data for actions 1, 2 and 3 are displayed in BatchWeb. The data is displayed in different fashions depending upon the display. For example in a property sheet the signature manifest data is displayed as property values; when the signed value is in a table an icon is included in the same cell that provides a hyperlink to call up a signature manifest pop-up window; and when a signed value is included in a chart a table containing the signature manifest data is provided below the chart. The signature manifest data for action 4 is displayed as part of the Report Template Manager Tool. This is also available for display on reports. The signature manifest data for action 5 may be included in the report output.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(2)	The **date and time** when the signature was executed; and	YES		Refer to Section B/11.50 (a) (1) above
(3)	The **meaning** (such as review, approval, responsibility, or authorship) associated with the signature.	YES		Refer to Section B/11.50 (a) (1) above
(b)	The items identified in paragraphs **(a)(1), (a)(2), and (a)(3)** of this section shall be **subject to the same controls as for electronic records** and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	YES		Refer to Section B/11.50 (a) (1) above
B/11.70	Signature/record linking			
	Electronic signatures and hand-written signatures executed to electronic records shall be **linked to their respective electronic records** to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	YES		Electronic signatures are linked to their respective electronic records in the Exaquantum/Batch database. The database is located in the Exaquantum/Batch server and is protected with Windows security thereby preventing records from being altered by ordinary means.
C/11.100	General requirements			
(a)	Each **electronic signature shall be unique** to one individual and shall not be reused by, or reassigned to, anyone else.	YES		Exaquantum/Batch utilizes Windows user name and passwords for electronic signatures. Exaquantum/Batch customers are responsible for the administration of Windows user accounts. Most regulated companies have policies and procedures to meet this requirement.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(b)	**Before** an organization establishes, assigns, certifies, or otherwise **sanctions an individual's electronic signature**, or any element of such electronic signature, the organization shall **verify the identity of the individual**.	N/A		Exaquantum/Batch utilizes Windows user name and passwords for electronic signatures. Exaquantum/Batch customers are responsible for the administration of Windows user accounts. Most regulated companies have policies and procedures to meet this requirement.
(c)	Persons using electronic signatures shall, **prior to or at the time of such use, certify to the agency** that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	N/A		Customers operating under the Part 11 regulation are responsible for determining when electronic signatures are to be used and for certifying to the FDA that the electronic signatures are intended to be the legally binding equivalent of traditional handwritten signatures.
(1)	The **certification** shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.	N/A		Customers operating under the Part 11 regulation are responsible for this submittal.
(2)	Persons using electronic signatures shall, **upon agency request, provide additional certification or testimony** that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	N/A		Customers operating under the Part 11 regulation are responsible for providing the additional certification or testimony to the FDA as required.
C/11.200	Electronic signature components and controls			

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(a)	Electronic signatures that are not based upon biometrics shall:			
(1)	Employ **at least two distinct identification components** such as an identification code and password.	YES		Exaquantum/Batch electronic signatures use Windows user name and password for identification of individuals.
(i)	When an **individual executes a series of signings during a single, continuous period** of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	YES		Exaquantum/Batch requires both user name and password be entered for each signature. If a series of actions requiring an electronic signature are taken both components of the signature must be entered for each signature.
(ii)	When an individual executes **one or more signings not performed during a single, continuous period** of con-trolled system access, each signing shall be executed using all of the electronic signature components.	YES		Exaquantum/Batch requires both user name and password be entered for each signature.
(2)	Be used only by their genuine owners.	YES		Exaquantum/Batch uses Windows user name and passwords for electronic signatures. Exaquantum/Batch customers are responsible for the administration of Windows user accounts. Most regulated companies have policies and procedures to meet this requirement.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(3)	Be administered and executed to ensure that **attempted use of an individual's electronic signature by anyone other than its genuine owner** requires collaboration of two or more individuals.	YES		Exaquantum/Batch uses Windows user name and passwords for electronic signatures. Exaquantum/Batch customers are responsible for the administration of Windows user accounts. Most regulated companies have policies and procedures to meet this requirement.
(b)	**Electronic signatures based upon biometrics** shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A		N/A Exaquantum/Batch does not use electronic signatures based upon biometrics.
C/11.300	Controls for identification codes/passwords			
	Persons who use **electronic signatures** based upon use of identification codes in combination with passwords **shall employ controls** to ensure their security and integrity. Such controls shall include:			
(a)	**Maintaining the uniqueness of each combined identification code and password**, such that no two individuals have the same combination of identification code and password.	YES		Exaquantum/Batch customers are responsible for maintaining this uniqueness. Most regulated companies have policies and procedures to meet this requirement. Windows's requirement that user account names be unique can be used to meet this requirement. Customers are recommended to disable instead of deleting a Windows user account. This will prevent multiple individuals from using the same user account name over time.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(b)	Ensuring that **identification code and password issuances** are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	YES		Exaquantum/Batch customers are responsible for Windows user account maintenance. Most regulated companies have policies and procedures to meet this requirement. Windows standard security features can be used to meet this requirement.
(c)	**Following loss management procedures** to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	YES		Exaquantum/Batch customers are responsible for Windows user account maintenance. Most regulated companies have policies and procedures to meet this requirement.
(d)	**Use of transaction safeguards** to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	YES		Exaquantum/Batch customers are responsible for Windows security settings. Most regulated companies have policies and procedures to meet this requirement using Windows domains. Windows security can be used to lockout accounts after a user-defined number of failed login attempts. This combined with the logging of successful and failed log-ins can help meet this requirement.

Section #	Requirement	Meets Requirements?		Compliance/Documentation/Comments
		Yes	No	Exaquantum/Batch
(e)	**Initial and periodic testing of devices**, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	N/A		N/A Token cards or other devices that generate identification code or password information are not currently used.

Yokogawa:

Yokogawa's global network of 19 manufacturing facilities, 85 affiliate companies and over 200 sales and engineering offices span 40 countries. Since its founding in 1915, the US$4 billion company has been engaged in research and innovation of the highest order, securing more than 8,000 patents and registrations, including the world's first DCS and digital flow and pressure measurement sensor. Industrial Automation Systems, test and measurement systems and information services are a core business of Yokogawa. For more information about Yokogawa Electric Corporation please visit their website at www.yokogawa.com

Stelex:

Stelex, a Xybion Company, provides software solutions and services to improve business processes for regulated industries. Stelex has the expertise, strategies and technology to help clients mitigate risk, enhance productivity and increase profitability. As a client-centered organization, Stelex tailors solutions to meet the requirements and achieve the business goals of our clients. Stelex is a division of Xybion Technology Solutions, a privately held company that is wholly owned by the Xybion Corporation which provides software and consulting services to life sciences, manufacturing, transportation, financial and other industries. To learn more about Stelex visit their website at http://www.stelex.com.

July, 20 2010

Revision Information

Title : Achieving 21 CFR Part11 Compliance using Exaquantum/Batch Authored by Stelex
Manual No. : TI 36J04B11-01E

July 2004/1st Edition
Newly published
May 2005/2nd Edition
Revision according to R1.02 release
July 2010/3rd Edition
Revision according to R2.50 release

Written by Yokogawa Electric Corporation
Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, Japan